Maritime Science and Technology Experimentation Capability Project

Maritime Capability Evaluation Laboratory (MCEL) Data Centre Requirements

Bassem R. Mikhael

Simpire Incorporated
813 Clearbrook Dr.
Ottawa, Ontario
K2J 0B3

Prepared By:
Acron Engineering
1600 Carling Ave, Suite 620
Ottawa Ontario
K1J 1G3
Simpire Incorporated, Sub-Contractor
Acron Document: 2012-0002
Contract Project Manager: Scott Arbuthnot, 613-236-6645
PWGSC Contract Number: W7707-125488/001/HAL
Contract Scientific Authority: Mark Hazen
DRDC Atlantic Research Centre
902-426-3100 (176)

The scientific or technical validity of this Contract Report is entirely the responsibility of the Contractor and the contents do not necessarily have the approval or endorsement of Defence R&D Canada.

DRDC-RDDC-2014-C54
August 2014

Abstract

The MCEL is the third component of the Maritime Science and Technology Experimentation Capability Project. MCEL is a “virtual shipyard” that supports a number of simulated maritime vessels (synthetic platforms). Among its key uses will be the development of experiments utilizing both new and existing synthetic platforms within a synthetic environment where these platforms can be evaluated in combat scenarios. Additionally, the MCEL will also be used for the evaluation of human subjects within these scenarios over a variety of performance indicators. This report focuses on investigating the implementation of data centre aspects of the MCEL as outlined in the statement of operational requirements. We first report on the applicability of the TIA-942 Data Centre Standard and other standards as they relate to the MCEL. We then present a suggested configuration for the MCEL with respect to network, simulation and other hardware components. This configuration allows for operation on networks of multiple security caveats and provides for the simultaneous operation of two synthetic platforms. From this configuration, estimates for power and thermal load are derived and presented. In addition, we present a number of strategies for noise reduction within the various rooms of the MCEL facility.

Executive summary

Maritime Science and Technology Experimentation Capability Project: Maritime Capability Evaluation Laboratory (MCEL)

Bassem R. Mikhael; DRDC-RDDC-2014-C54; August 2014.

Introduction or background: The goal of the MCEL project is to address the issue of rapid degradation and obsolescence of various combat systems by shifting development from operational units to a land-based facility where rapid capability evolution may be achieved at a reduced cost [1]. With this in mind, the MCEL's primary focus will be the acceleration and further development of currently in-service maritime combat systems as well as the trial of simpler prototypes in a realistic environment. In addition, MCEL can be used to evaluate human factors issues and operations centre capabilities in an experimental setting. In this study we investigated a number of the aspects associated with the development of the MCEL with respect to network topology, hardware configuration, electrical requirements and system cooling.

Results: An initial breakdown and configuration of all of the hardware for the MCEL based upon various industry standards and best practices was determined. Our design initially divides the hardware into two main categories: (i) network equipment and (ii) simulation equipment. We then further divide the simulation equipment on the basis of its membership in an enclave, simulation platform or test network. This was deemed appropriate based upon the logical groupings provided within the MCEL statement of operational requirements.

Taken together our results showed that the MCEL could be established in a facility providing it with a power source of 78kWh and cooling on the order of 22.04 tons of air conditioning. Using this strategy, we found that all of the equipment for the MCEL could be contained in 11 racks and our recommendation is that each rack be provisioned with at least a single KMM. Finally, our research investigated various strategies to reduce the noise of the MCEL. These strategies included the use of raised floors as well as sound insulation in the ceilings of particularly noisy rooms.

Significance: The MCEL will provide the Canadian forces with a unique capability for testing and evaluation of operations centre combat systems. This work provides baseline estimates of data centre requirements for the options analysis.

Future plans: As mentioned, the MCEL project is currently in its options analysis phase. This work will provide an excellent design guideline for development once MCEL project reaches its implementation phase.

This page intentionally left blank.

This page intentionally left blank.

Table of contents

List of figures

List of tables

1 Applicability of the TIA-942 Standard and Other Relevant Standards

1.1 The TIA-942 Data Centre Standard

The TIA-942 Data Centre Standard was developed with the purpose of providing requirements and guidelines for the design and installation of a data centre or a computer room (*reference TIA-942 doc). The standard was produced as a joint effort by a number of TIA TR-42 subcommittees in concert with over 60 organizations from the telecommunications industry. The Standard was designed with a number of key purposes in mind. Some of these are listed as follows:

1. Promote the design of the data centre early in the process of the overall building construction.

2. Providing guidelines for data centre design and related facilities including server rooms, computer rooms and network rooms.

3. Providing specifications for data centre cabling infrastructure, systems and pathways with respect to media types and lengths.

4. Providing guidelines for establishing data centre redundancy.

5. Defining a standard telecommunications infrastructure for data centres.

6. Defining a standard for classifying data centres into various tiers as opposed to previous proprietary methods.

While the TIA-942 was developed from the perspective of telecommunications, about fifty percent of the content deals with specifications relating to the building/facility that will actually hold the data centre. This makes the Standard an invaluable tool for planning all aspects of a data centre development project. The Standard specifies two types of specification criteria: mandatory and advisory requirements. Mandatory requirements are referenced by the word “shall” whereas advisory requirements are referenced with the words “should”, “may” or “desirable”. Mandatory requirements are those that establish the minimum acceptable requirements. Mandatory criteria deal with requirements relating to protection, performance, administration and compatibility of the data centre in question. Advisory criteria are those which are expected to enhance the performance of the cabling system in all of its anticipated uses. The TIA-942 also includes a series of informative annexes (A-H). These annexes provide useful information on a number of topics relating to the establishment of the data centre but are not specifically part of the standard itself unless so noted within the text itself. It should be noted that data centres use a number of transmission protocols whose distance restrictions may be less than those proposed by the Standard. While these proprietary restrictions should be adhered to in the final design, the Standard recommends that both proprietary and standard cabling be consolidated into a single structured cabling system.

1.2 Applicability of the TIA-942 Data Centre Standard and other relevant standards.

Because the TIA-942 standard can be used as a planning, design and evaluation tool for data centres, its applicability to the MCEL project is obvious. However, the MCEL project is currently in its options analysis phase and as such, the focus of the current effort should be the gathering of requirements. The intention of this document is to outline an inaugural set of requirements for the MCEL project. The design and development of the MCEL project is to be a collaborative effort and will require the cooperation of staff from DRDC Atlantic, local engineering staff from the base as well as DIMTPS personnel. All parties have critical elements to play in ensuring the design meets DRDC Atlantic's objectives as well as DND objectives and legislative requirements. DRDC, as the requestor, needs to agree to any proposed design and thus has the ultimate responsibility to ensure that the design meets their requirements. Local engineering staff from the base, as the agency providing real estate and all necessary support services, needs to ensure that building design and support services are designed to integrate into the local base services and can be properly provisioned. Design and subsequent installation of necessary electrical, HVAC, fire suppression, lighting and other systems can be completed by combinations of local engineering and contractor personnel. Ultimately, DIMTPS staff will be responsible for ensuring that relevant standards and best practices (including DIMTPS own best practices) for the design of the data centre are followed. It will be their role to determine the applicability of the TIA-942 Standard to the MCEL project along with other relevant standards and best practices guidance. DIMTPS, after thoroughly understanding the MCEL data centre requirements, will create a Project Directive that will detail the data center design and ensure it is in compliance with Government of Canada and industry standards. Some of the standards relevant to a data centre within the Government of Canada are:

1. Canadian Electrical Code Book, 2002
2. INFOSEC 601 (Classified)
3. Standard 1606-4000
4. DND Information Technology Security Policy
5. ANSI/TIA/EIA-569-A
6. ITSG-11
7. TBITS 6.9 3.4.3
8. NSTISSI No. 7003, 1996
9. CAN/CSA-C22.2, 2006
10. CAN/CSA-T530, 2002
11. CAN/CSA-T527-94, 1994
12. CAN/CSA-S136-01, 2001

13. Quebec Provincial Fire Code, 2009

14. Fire Protection and Prevention Act, 1997

The DIMTPS Project Directive will detail among other items, the cable/fibre runs, the structured cabling hardware, location of all network drops, location of network racks, location of server racks, HVAC and power requirements.

2 Network Overview

One of the key enablers of the MCEL will be its connectivity to external networks and a robust internal test network infrastructure. External connections will allow the MCEL to collaborate and participate with various coalition partners at appropriate security levels, maintain connectivity to both DRDC and CF national networks, and the potential of a connection to unfiltered Internet access via an ISP. Internal-only connectivity will allow the MCEL to test configurations within a safe environment and within the proper security caveat. Additionally, the MCEL should have a management LAN to provide out of band management to its IT equipment as needed.

2.1 Recommended External WAN Connections

The following details the list of recommended external wide area network connections for the MCEL.

1. **CFXNet** – CFXNet has become the de-facto M&S network within the CF. CFXNet is maintained by CFWC who are both the OA and TA for CFXNet. CFWC connects to Coalition partners via CFBLnet (CFWC maintains a persistent CFXNet-CFBLNet connection at Arlington VA) and will shortly have a persistent connection to the US JTEN at Peterson AFB. CFXNet has a variety of security enclaves ranging from Unclass to Secret 2Eyes.

    a. **CFXNet Secret 2 Eyes** – As the RCN conducts many operational exercises with the USN, it is assumed that there will be a requirement for a classified enclave operating at the Secret 2Eyes caveat. MCEL staff can expect to assist in configuration and maintenance of this connection.

    b. **CFXNet Secret 4 Eyes** – A Secret enclave at the 4Eyes caveat is assumed to be a requirement. CFWC is advancing, along with the other partner nations, a proposal to stand up, on a JTEN backbone, a persistent 4Eyes coalition enclave. This enclave will allow the MCEL to conduct experiments and exercises with Coalition partners at the Secret level. MCEL staff can expect to assist in configuration and maintenance of this connection.

    c. **CFXNet Unclass -** An unclassified enclave would allow the MCEL to conduct/participate in experiments/exercises with any other CFXNet unclassified site and/or other nations that can be reached via CFXNet/CFBLnet connectivity. MCEL staff can expect to assist in configuration and maintenance of this connection.

    d. **Other** – M&S is still at a nascent stage within many countries. While DND is past this stage it still does not have a robust national M&S infrastructure and processes. Most CF M&S initiatives, at the Secret level, are limited to either 2 or 4 Eyes initiatives. Over time this will change and thus the MCEL should track this progress. One can expect to see a demand start to germinate for NATO Secret in the coming years. The network & server rooms should provide the physical capability for but not actually be provisioned with this capability at this time.

2. **DRENet** – DRDC's internal WAN. MCEL staff should not expect to be involved in the configuration and maintenance of this connection.

3. **DWAN** – DND's internal WAN. MCEL staff should not expect to be involved in the configuration and maintenance of this connection.

4. **CSNI** – DND's classified operational network. MCEL staff should not expect to be involved in the configuration and maintenance of this connection.

5. **External Internet** – it is recommended that the MCEL explore the possibility of having an external Internet connection. This resource would have to be carefully monitored and have very limited distribution. This resource has proven beneficial at similar installations for the downloading of security patches. Security patches are frequently prevented by firewalls as DWAN/DRENET system administrators do not allow executable files to be downloaded. Additional benefit is the ability to download larger files that would be prevented via DWAN/DRENET. This does open a potential security breach and so a file scanning policy and process must be implemented to ensure that any files downloaded are scanned prior to being transferred to an operational/test network.

2.2 Recommended Internal LAN Connections

The following details the list of recommended internal LAN and corresponding connections for the MCEL.

1. **Secret 2 Eyes M&S Operational LAN**. This LAN would be connected externally to the CFXNet 2Eyes enclave. This LAN will be controlled and configured by MCEL staff.

2. **Secret 4 Eyes M&S Operational LAN**. This LAN would be connected externally to the CFXNet 4Eyes enclave. This LAN will be controlled and configured by MCEL staff.

3. **Unclass M&S Operational LAN**. This LAN would be connected externally to the CFXNet Unclass enclave. This LAN will be controlled and configured by MCEL staff.

4. **DRENET LAN**. This LAN will be connected externally to the DRENET. This LAN will be configured and maintained by DRENET staff.

5. **DWAN LAN**. This LAN will be connected externally to the DWAN. This LAN will be configured and maintained by DWAN staff.

6. **CSNI LAN**. This LAN will be connected externally to the CSNI. This LAN will be configured and maintained by CSNI staff.

7. **2EYES Test LAN**. This LAN will not be connected externally. This LAN will allow MCEL staff to test Secret 2Eyes configurations within a safe environment. All configuration changes to the Operational 2 Eyes LAN should be trialed in this environment first. This LAN should have the ability to replicate an external site and thus will require additional network equipment compared with the Operational 2 Eyes LAN. This LAN will be controlled and configured by MCEL staff.

8. **4EYES Test LAN**. This LAN will not be connected externally. This LAN will allow MCEL staff to test Secret 4Eyes configurations within a safe environment. All configuration changes to the Operational 4 Eyes LAN should be trialed in this environment first. This LAN should

have the ability to replicate an external site and thus will require additional network equipment compared with the Operational 4 Eyes LAN. This LAN will be controlled and configured by MCEL staff.

9. **Unclass Test LAN**. This LAN will not be connected externally. This LAN will allow MCEL staff to test Unclass configurations within a safe environment. All configuration changes to the Operational Unclass LAN should be trialed in this environment first. This LAN should have the ability to replicate an external site and thus will require additional network equipment compared with the Operational Unclass LAN. This LAN will be controlled and configured by MCEL staff.

10. **Management LAN**. This LAN is an OOB Management LAN for MCEL System Administrators. This LAN will allow System Administrators to conduct certain administrative functions on connected equipment without impacting ongoing operational activities. These specific administrative activities could include:

    a. Powering on/off servers – if servers have the applicable maintenance channel (e.g. HP – ILo interface, Dell – iDracs interface).

    b. Imaging servers – utilizing a tool like Symantec Ghost

    c. Adjusting BIOS.

    d. Performing software updates – i.e. Windows Update Server

    e. Gaining access to the Console server for network equipment

The OOB Management LAN is an internal only LAN that connects IT equipment irrespective of caveat. This has been done within DND however it will require care in planning, documentation and implementation.

2.3 Test Local Area Networks (LANs)

Implementation of the Test LANs should be in parallel with the operational LANs. It is possible to reduce the number of Test LANs as no classified data is stored on the network equipment (routers/switches) and thus the MCEL can make do with less Test LANs. The impetus for the number of Test LANs is the utilization rate of the operational LANs and the frequency/amount of testing that is required. One would expect to see both of these factors increase over time as the MCEL reaches maturity and, at this point, it is expected that the MCEL will require a Test LAN for each of its operational LANs.

3 Network and Simulation Equipment Considerations for the MCEL

3.1 Network Equipment

There are five network/server room groupings that have been identified. These groupings are:

1. Telecommunications
2. Unclassified Network
   a. CFXNet Unclass (main feed switch, firewall, router)
   b. DWAN (2 x switch)
   c. DRENet (2 x switch)
   d. Internal Test Network (3 x router)
3. Classified Network
   a. CFXNet 2 Eyes (Taclane, firewall, router)
   b. CFXNet 4 Eyes (Taclane, firewall, router)
   c. CSNI (Taclane, switch)
   d. Internal Test Network 2 Eyes (3 x router)
   e. Internal Test Network 4 Eyes(3 x router)
4. Unclassified Processing - Server Room
   a. Servers for CFXNet Unclass (and switch(es))
   b. Servers for Test Network Unclass
5. Classified Processing – Server Room
   a. Servers for CFXNet 2 Eyes (and switch(es))
   b. Servers for CFXNet 4 Eyes (and switch(es))
   c. Servers for Test Network 2 Eyes (2 x switch)
   d. Servers for Test Network 4 Eyes (2 x switch)

We have not looked at the Telco requirements for the MCEL facility however the facility will require a Telco closet. Some facilities have a joint Unclass network room which will include Telco and the unclassified network equipment. If this turns out to be the case at the MCEL, and this determination is part of the design process, then we would recommend that a separate classified network room be established. Additionally, there will be a requirement for server room(s). It is possible to put both classified servers and unclassified servers within the same room provided the CF security regulations are adhered to. The separation distance is not onerous and can be established with rack separation provided this is highlighted during the design process. For ease of management of the servers we recommend that this solution be sought.

All network equipment has been gathered into one logical grouping for ease of review.

3.2 Simulation Equipment (per Enclave)

We recommend that the capabilities detailed in Table 2 be provisioned on a per enclave basis as these are services that can support multiple simulations irrespective of numbers of SPs participating. There may be some specific configurations required to support multiple simulations. The MCEL technical staff may find it easier to provide some of these capabilities on a per SP basis. This has an increased hardware cost however it is less onerous from a configuration perspective. As an example, vice running a single Chat server where configuration prevents a participant in Simulation A from having access to Simulation B's Chat rooms, it may be easier to have separate Chat servers for each simulation. Ultimately this should be the purview of the MCEL's Tech staff.

3.3 Simulation Equipment (per Test Network)

We recommend that the capabilities detailed in Tables 3-5 be provisioned within the Test network and that each test network be laid out in a similar construct and that there is a single test network per security classification level. Having a test network per security enclave will significantly reduce the risk of inadvertently exposing classified information to a network of a lower security classification. Additionally, it will allow multiple tests of differing security caveats to occur. Each test network contains 3 routers – 1 representing the MCEL local site, 1 representing a distributed site, and the last router representing the WAN cloud. Additionally each test network contains 2 switches – 1 switch per site. This construct will allow the MCEL to test local configurations, at the appropriate security classification, as well as testing impacts of configurations under a simulated WAN construct.

3.4 Simulation Equipment (per SP)

We recommend that the capabilities detailed in Table 6 be provisioned within each SP as their capabilities are primarily focused on a specific SP. This does not preclude these capabilities from being established at the enclave level if that capability is subsequently determined to best reside there.

3.5 Overarching Considerations

We have detailed the requirements for an SP separate from those that are enclave specific. We fear that this could possibly overlook some real world constraints and so encourage the MCEL staff to use this document as a reference to encourage greater definition of their requirements as they move forward with this project. An SP cannot easily move across caveats without significant effort at the technical level. It is a bit simplistic to think that merely changing hard drives will allow movement of IT equipment across security caveats. While this may be feasible it does behove the IT staff to have local ISSO approval to conduct this type of migration and that this approval contain evidence that there is no residual data stored anywhere within the IT equipment. We believe that is easier to have SPs assigned to each security enclave. The number of SPs per security enclave would need to be determined by MCEL staff and appropriate adjustments to IT equipment and follow-on impacts to power and air conditioning assessed. Building in flexibility is paramount to success beyond implementation. While we calculated the necessary number of servers required to stand-up the MCEL based on our experience and inputs received, we feel that the MCEL needs to be prepared to grow. This growth, while specifically geared to adding computing power, reaches into power and air conditioning. Design should include the ability to either have excess power already in place or easily added. Air conditioning should be provisioned for immediate requirements plus foreseeable growth. Further, the air conditioning design should allow for growth of capacity without a complete re-build/overhaul.

4 Suggested Equipment Breakdown in the Design of the MCEL

4.1 Network Equipment (CFXNet)

Our recommendation is that the MCEL start with three simulation networks and three corresponding test networks. With that in mind, it is our assertion that using a similar network construct and similar equipment across these networks will reduce training costs, network stand-up time and follow-on network integration activities. The CFXNet will terminate within the MCEL at a CFWC supplied switch. Utilizing Cisco's 3 Layered network model[2], this switch would be the distribution layer. This distribution layer switch will have 3 ports activated on it (beyond the uplink port); 1 switch port for the Unclass enclave, 1 switch port for the 2Eyes enclave and 1 switch port for the 4Eyes enclave. This switch will be located within the telco /Unclass network room.

The distribution layer switch's Unclass switch port will connect to the Unclass firewall while the 2Eyes and 4Eyes switch ports will connect to their respective TACLANEs located in the classified network room. The Unclass firewall will be located in the Unclass network room while the 2Eyes and 4Eyes firewalls, connected directly to their respective TACLANEs, will be located in the classified network room. These firewalls should be configured as zone-based firewalls. These firewalls can be configured with a fairly simple 3 zone configuration[3]. The outside interface would be in an untrusted zone, the web server and ftp server could be set up within a DMZ, while all the other servers and PCs would be set up within a trusted zone. The inside facing interface of the firewall will connect to a router which should also be located within their respective network room.

The router selected should have the capabilities similar to a Cisco 2921 ISR. These capabilities include, with the appropriate IOS provisioning, VOIP (Cisco Unified Communications Manager Express) with an ability to handle 100 local phones. If the router was also provisioned with a DSP module then additional features of VOIP (e.g. multi-party conferencing) could also be enabled. The router will subsequently connect to a single access switch that will provide the bulk of the connectivity to the servers and client workstations on each CFXNet enclave.

Prior to discussing the capabilities sought in the access layer switches, it is prudent to discuss VOIP as this capability does impact the abilities required of the access switches.

There are 2 options to discuss regarding VOIP phones. It is possible to use a soft phone which is a software based phone. This will require any stations using a soft phone to run the software that will create a phone emulation on their computer screen. This emulation is then manipulated with a mouse or touchscreen and the corresponding inputs/outputs are provided through a headset and/or speakers & microphone. These soft phones are typically used with USB headsets. If hard VOIP phones (i.e. Cisco 7961G) are preferred then there are several decisions to be made. If the number of network drops is a limiting factor at each station then it is possible to connect the station's PC to the phone and then the phone to the network drop. In this instance it is important to ensure that the PC switch port on the back of the VOIP phone is a gigabit Ethernet switch port. If the number of network drops is not a factor then both the station's PC and VOIP phone can have their own network drop.

There are two mechanisms to provide power to the phone. One mechanism is to use a standard power brick that will utilize one power outlet at the station. Another mechanism is to use POE. POE provides the phone with its required power through the network drop. This necessitates that the network drop is copper Ethernet, thus this is only used on Unclass networks, and that the switch is capable of providing POE. Classified networks tend to use fibre for their distribution within buildings and so POE is not traditionally available on the classified enclaves. Additionally, VOIP phones tend to only have a copper Ethernet connection and so a media converter is required to modify the signal between copper and fibre. Some of these media converters can provide POE and thus, if one of these is used, one less power outlet at the station will be required.

It is expected that the Unclass distribution system will be copper so the access switch can have copper only switch ports. This switch should be located in the server room along with the patch panels that run out to the various rooms. The classified enclave's access switch will require fibre switch ports although it should also have a sizeable number of copper switch ports as the servers can connect via copper provided the approved shielded cables are used. These switches should be located in the classified server room.

A Cisco 4506 is a suggested example of a singular access layer switch that could provide access to the network for the majority of users. In the event that additional switching was required then any additional switches could be interconnected with this main distribution switch. A Cisco 4500 series switch comes in different versions and has different numbers of line cards. Each line card contains up to 48 switch ports and so the specific model is directly related to the expected number of users (i.e. Unclass users on the floor and Unclass servers). Additional switches will be necessary for the test network and may be needed on the operational network depending upon changing configurations. A switch that has the ability to utilize SFP transceivers will offer the MCEL greater flexibility to tailor configurations based on requirements especially on the Test LANs. SFPs are removable transceivers that change the switch port from a Copper Gig switch port to a Multi-Mode Fibre switch port merely by swapping the SFP. Cisco does produce Catalyst 3750 switches that have all switch ports designed for use with SFPs.

The following outlines the types and quantities of the recommended network hardware/capabilities for standing up the MCEL on the CFXNet:

1 x Firewall/IPS per enclave (Cisco 5520)

1 x Router per operational enclave (Cisco 2900 Integrated Services Router)

VOIP capability

Multi-VLAN capability (router and switches need to be VLAN capable as VLANs will be needed for traffic segregation however some of this segregated traffic can be brought back together when required[4])

3 x Routers per test enclave (Cisco 2900 Integrated Services Router)

1-3 Switches per enclave (1 Cisco 4500 switch and/or 2-3 Cisco Catalyst 3750 switches)

Single 4500 switch can have multiple line cards (depending on model). Line cards can support different capabilities - POE, 100FX, Gig SFP etc. These multiple capabilities are important not only for the planned implementation of capabilities but also for future growth.

May require 1-2 Cisco Catalyst 3750 switches to provide the required capabilities required of each enclave. This is dependent upon the number of network drops the MCEL will have and the model and capabilities of the 4500 switch provisioned.

2 Switches per test enclave (i.e. Cisco 3750 switches)

The interconnection of these components in the suggested configuration is outlined in Figure 1.

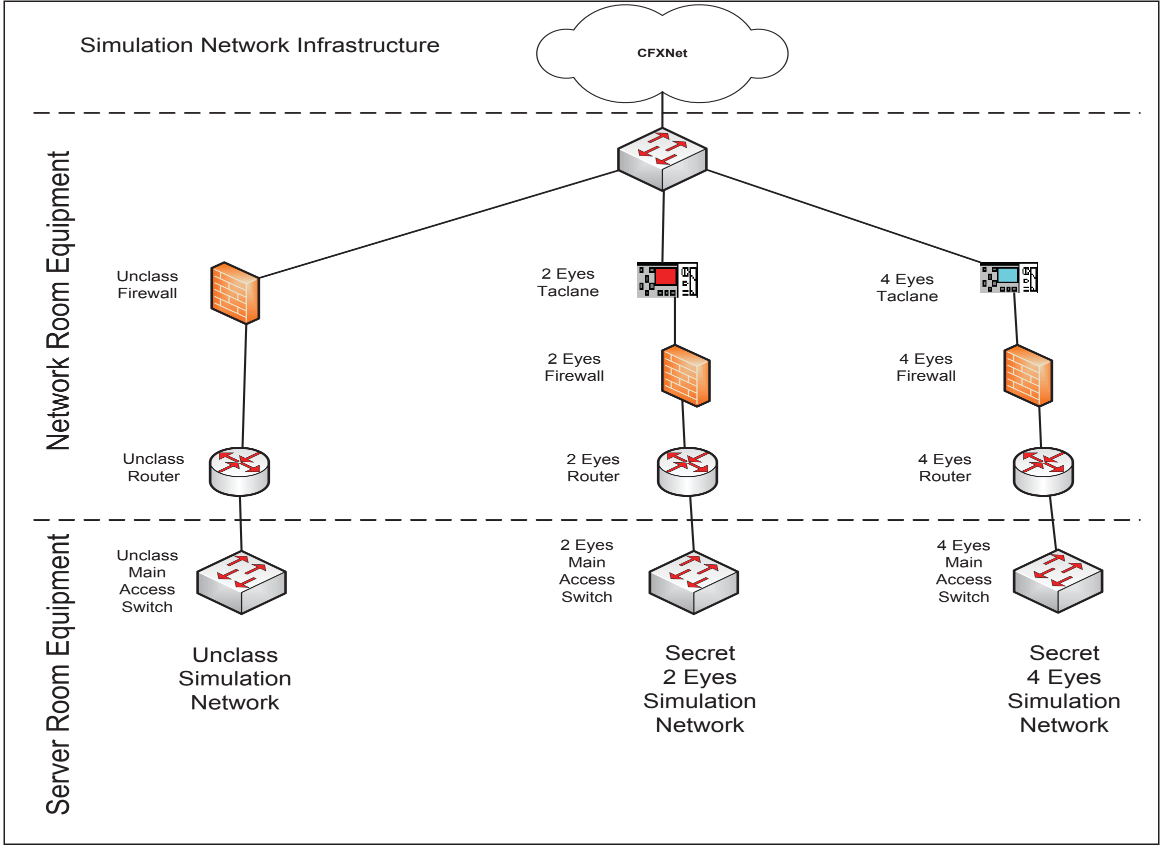

Simulation Network Infrastructure
CFXNet
Network Room Equipment
Server Room Equipment
Unclass Firewall
2 Eyes Taclane
4 Eyes Taclane
2 Eyes Firewall
4 Eyes Firewall
Unclass Router
2 Eyes Router
4 Eyes Router
Unclass Main Access Switch
2 Eyes Main Access Switch
4 Eyes Main Access Switch
Unclass Simulation Network
Secret 2 Eyes Simulation Network
Secret 4 Eyes Simulation Network

Figure 1: Proposed Network Infrastructure for the MCEL Project

4.2 Network Equipment (Non-CFXNet)

The switches required for DRENet, DWAN, and CSNI will be determined by the organizations responsible for those networks on base. Whether the MCEL can recycle existing hardware for those switches or whether the MCEL will have to fund the acquisition of those to be specified switches is unknown at this time. We have utilized Cisco 3750 switches as examples for power and air conditioning determinations. The following outlines the types and quantities of the recommended network hardware/capabilities (Non-CFXNet) for standing up the MCEL:

1-2 Switches for DRENet. The number depends upon the number of DRENet drops desired for the building.

1-2 Switches for DWAN. The number depends upon the number of DWAN drops desired for the building.

1 Switch for CSNI. CSNI drops are hardwired solely for CSNI and the switch necessary is dependent upon the number of CSNI machines desired within the MCEL.

4.3 Other Network Equipment

Console Server. To provide the ability to manage all network equipment from positions external to the network rooms, a console server(s) is required. It is recommended that a console server be added to the classified networking room as there is significant equipment that can be connected via a console server (routers, firewalls). Adding a console server to the unclassified network room would provide the same flexibility although there will be significantly less equipment within that room.

Management Switches. To provide the ability to utilize the lights-out management capability of modern servers, it is recommended that switches be provided for this capability. These switches can be primarily copper although they will require a fibre uplink so that the management station(s) can be deployed to the MCEL floor.

4.4 Cryptography Equipment

Both CSNI and CFXNet utilize TACLANEs as the cryptographic equipment for encrypting/decrypting data passed on classified enclaves. Acquisition of the respective Taclances will be identified during the RFC process and captured within subsequent Project Directives. The MCEL project can expect to be required to fund the acquisition of TACLANES but not actually be involved in the actual procurement. The following lists the type and quantity of the needed cryptographic equipment for the MCEL:

1 **Taclane per classified enclave**. The current standard is the Micro Taclane. General Dynamics does produce a GigE encryptor although it is not currently a common encryptor within the CF. TACLANEs are necessary for the following caveat connections:

- CFXNet 2 Eyes
- CFXNet 4 Eyes
- CSNI

The establishment of other classified caveats will occur in due course. But at this time, we do not recommend acquisition of additional TACLANEs until this actual requirement is identified.

4.5 Servers

The server infrastructure of the MCEL represents the actual simulation capability of the MCEL. The following lists the types and quantities of servers/capabilities recommended for the MCEL project:

Digital Voice – 2 ASTi T4 servers per simulation platform, 1 server per test network

- Digital radio emulation is recommended to allow simulation of the radios onboard naval platforms. There are a variety of potential products that can meet this capability however we have selected, as an example, the ASTi Telestra 4 as this is a CASE supported product.

Underwater Telephone – 1 server per simulation platform, 1 server per test network.

- Underwater telephone emulation is recommended on a per platform instantiation to allow simulation of the full complement of communication capabilities available on any naval platform. There is potential for the Telestra 4's to be able to emulate this capability although that has not been specifically explored. A single server has been allocated per simulation platform in the event the Telestra 4's can not emulate the underwater telephone capability.

Licence server (IGs, Mak, etc). – 1 Server per enclave and per test network

- Some simulations tools take advantage of licensing schemes that allow licenses for their software to be allocated dynamically to machines. This scheme, much like a library, allows these licenses to be checked in and out automatically through a license server. The MaK product suite of simulation tools, which is supported by CASE, can use this scheme.

Gateway (DIS-HLA) – 1 Server per simulation platform, 2 total for the 3 test Networks

- Two protocols (DIS & HLA) are the most prevalent simulation protocols in use today. DIS is clearly the most prevalent protocol however support for the HLA protocol is important. Having the ability to pass simulation traffic between these two protocols is critical to ensure inter-operability with legacy & emerging equipment, with fellow CF units and with Coalition partners. A DIS-HLA gateway will allow the MCEL to pass traffic from one protocol to the other protocol and vice-versa.

RTI Exec/Forwarder – 2 Servers per enclave, 4 servers total for test networks

- The MaK HLA implementation allows the RTI Exec and Forwarder to be separated for network optimization. An RTI Exec can run multiple Federations.

Filter – 1 Server per Simulation Platform, 2 for test networks

- DIS is a Broadcast based protocol and so it can generate significant traffic. A filter mechanism will allow the MCEL to control the amount of traffic that is being forwarded (either to a resident simulator or to any external agencies) by applying a rule set for data forwarding. If the data does not meet the applicable rule set then the traffic is not forwarded.

Logger – 1 Server per Simulation Platform, 2 for test networks

- Logger software will allow the MCEL to record the entirety of a simulation event. This recording can then be used for analysis, for playback during an AAR, and maintained for historical purposes. Some typical logging software includes MaK Logger and Red Sim DIS PDU Logger.

Software Router (DIS) – 1 Server per enclave, 2 for test networks

- DIS is a Broadcast based protocol and so it is not forwarded by routers natively. This capability can be enabled on the router however it has the potential to significantly impact the router's performance due to the volume of traffic and the CPU capabilities of the router (router's CPUs tend to be significantly less than servers). A more scalable option is to utilize a server based program to convert Broadcasts to either a multicast or unicast data packets for furtherance by the router. These programs already exist within the CF inventory as a GOTS product.

CGFs - 1-3 servers per Simulation Platform, 2 servers per test network

- Depending upon the experimentation/simulation that is being run, the MCEL may require several CGFs. Different CGFs have different capabilities and differing levels of realism incorporated into their entities

Simulation Viewers/Common Operating Picture/Command & Control - 1-4 Servers per Simulation Platform, 8 total for test networks

- Depending upon the experimentation/simulation there will likely be a requirement to view specific entities/parts of the simulation and/or the overall simulation. This capability may not be resident within the selected CGFs and so would require additional servers to support. Some of these tools are PC based (MaK VR-Vantage and Mak PVD) whereas some of these tools are server based (GCCS-M)

Replication Servers (estimated 10 – 15 servers) per Simulation Platform, 30 for test networks

- This capability is not as tightly defined as the above specific requirements. This requirement is summarized as how much computing is required to replicate the maritime platform's combat management and associated systems. This is an estimate only.

Web Server – 1 Server per enclave, 1 server for test network.

- It is recommended that the MCEL maintain a persistent connection to each enclave on CFXNet. Having a web server on each enclave will afford the MCEL the ability to promote its activities, calendar, and contacts to all other users of each simulation enclave.

Chat Server – 1 server per enclave, 1 server for test network.

- Each enclave should have its own chat server to allow all participants within that enclave to utilize this resource. If both simulation platforms are running in discrete simulations then you can configure the specific chat rooms to only allow specific users and thus segregate users based on simulation platform.

E-mail/Exchange Server – 1 server per enclave, 1 server for test network.

- Each enclave should have its own e-mail/exchange server to allow all participants within that enclave to utilize this resource.

FTP server – Use an existing server for this capability.

- The File Transfer Protocol server will allow files to be transferred over the network. The FTP server can reside on any of the enclave assigned servers (i.e. e-mail server).

4.6 Storage

It is recommended that 1 single storage server solution be provisioned within each enclave and that the capacity of this solution be between 6-12 TB (terabytes). Storage will be of benefit on the test networks although initially this can be accomplished by utilizing the storage capabilities of the servers and PCs. Some specific requirements of this storage solution are as follows:

This storage should be able to be portioned between general user space and system administrator specific storage space.

Flexibility to expand as storage requirements grow.

4.6.1 Storage Area Networks

SANs operate using blocks of data and thus allow for rapid movement of data between servers and the SAN. SANs use a special networking protocol, Fibre Channel, and thus require dedicated switches and fibre for their network connectivity. Typically SANs are used in facilities where massive amounts of data are being stored and accessed and the integrity and access performance are critical. SANs are for use by servers and not by users. SANs are more complex and so there is a learning curve and associated cost in the implementation to ensure that system administrators are familiar with their operation and upkeep. This initial cost should not be viewed as a negative item. If the requirement is for a SAN then the training cost is merely a small component of the overall cost.

4.6.2 Network Attached Storage

NASs serve data as files and so it is more intuitive to users as this is the format to which they are most accustomed. NASs operate over Ethernet and so do not require any additional hardware. A NAS will compete for bandwidth and so moving large files should not occur whilst a simulation is underway on the same network.

4.6.3 SAN vs. NAS

SANs are currently faster than NASs however we can expect to see the performance gap continue to shrink as common Ethernet speeds push the 10Gigbit limit and beyond. Many small data centers use NAS especially if their data storage requirements are not large. Additionally, many vendors are starting to offer a hybrid SAN/NAS solution where files can be accessed via either mechanism. SANs can reduce the requirement for storage at each server. NASs provide a single repository for both users and servers albeit file based. While a NAS is not as quick as a SAN it is easier to set up and maintain. Further, a NAS utilizes a file structure that is already understood by novice and experienced computer users alike. A NAS is easily portioned so that contractors or other users have an accessible central drive.

4.6.4 Recommendation

There are strengths and weaknesses with either a SAN or a NAS solution and potentially the requirement is for both. While a SAN is technically superior in performance it comes with an overhead in design, maintenance, hardware and in flexibility. We do not envisage the data storage or throughput to warrant the additional overhead that a SAN would entail. We would recommend pursuing a storage solution that combines the strengths of both solutions. These hybrid solutions, typically called unified storage solutions, are continuing to evolve and offer the best path for both file and block storage. We would recommend a single control head and one bank of hard drives to start. Additional banks of hard drives could be added to specific control heads as the requirement arises. Actual storage available for initial installation will be a factor of price and the standard hard drive sizes available when the actual product is ordered. At this point we typically see initial arrays of approximately ***12 x 500Gb or 1Tb drives.***

4.7 Racks

The total number of racks required for this variation of the MCEL is eleven racks. Each of these racks should be provisioned with a KMM so that, if required, IT equipment can be worked on from the room where the rack is located. These racks are broken out within the previously described server/network room groupings:

- Telco/Unclass Network Room – One rack total for network equipment (one firewall and four routers) and one UPS. This equipment may be able to be integrated into telco racks however this would need to be coordinated during the design/procurement phase.

- Classified Network Room – Two racks total for network equipment and associated UPS. There would be two Firewalls and eight routers with their UPS. Depending on models of equipment chosen this could fit within one rack however two racks would afford an immediate opportunity for growth and would not impinge upon model selection.

- Unclass Server Room – Two racks total for the unclass server room. One rack is for the Unclass enclave equipment and one rack is for the Unclass Test LAN equipment and their associated UPS.

- Classified Server Room – Six racks total for the classified server room. Two racks for enclave equipment (2Eyes rack, 4Eyes rack), two racks for SP equipment (SP1 rack, SP2 rack) and two racks for Test LAN equipment (2Eyes Test, 4Eyes Test) and these racks associated UPS.

4.8 Future Growth

While we have documented our estimation for the number of servers required per enclave, it is critical that the design process take into account expansion. The network and server rooms (server room more so) must be designed with the capability to expand beyond this estimate. Size of the server and network rooms must be provisioned for future growth whereas power and AC must be designed to allow for expansion even if not specifically provisioned.

5 Power and Cooling Considerations for the MCEL Project

In this section we discuss the power and cooling considerations for the MCEL project and present an initial estimate for the electrical and air conditioning requirements of its components. This estimate is based upon the equipment breakdown given above (see Section "Suggested Equipment Breakdown in the Design of the MCEL") and the use of the HP C7000 Chassis for the server portion of the simulation equipment where no application specific server is defined (i.e. ASTi Telestra 4 platform for simulated radio communications). This platform was chosen as being representative as it permits the addition of up to 16 blade servers in a given chassis without increase in heat or consumption (i.e. 6 power supplies per chassis). When combined with virtualization technology, all server requirements as described in the given breakdown are met using less hardware than a comparable breakdown using a solution based on the Dell PowerEdge R610 server platform. A number of assumptions regarding this platform were made as follows:

Each HP C7000 Chassis will have a full complement of 6 power supplies providing for a total of 7200 Watts of power regardless of the number of Blade servers installed.

Each HP C7000 Chassis will ***initially***, not be more than half filled with Blade servers (i.e. 8) to allow for expansion as new requirements are identified.

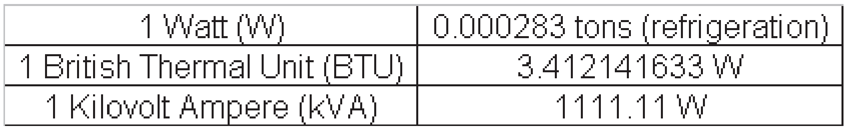
Each Blade server will be equipped with dual Intel Xeon x5680 processors (6 processor cores each), 96GB of RAM and an arbitrary amount of secondary storage as provisioned by the storage solution.

Each Blade server with the above configuration will therefore have the mathematical capacity to simultaneously run a maximum of 12, single core virtual machines with 8GB of RAM each.

Each Blade server will ***initially*** have no more than 8 virtual machines of the above configuration so as to allow for expansion when additional requirements are identified.

Power and cooling estimates are based upon manufacturer published specifications and industry standard conversion factors for unit harmonization. Table 1 gives a breakdown of all of the conversion factors used in this report.

Table 1: Unit Conversion Factors for Power and Cooling Estimates



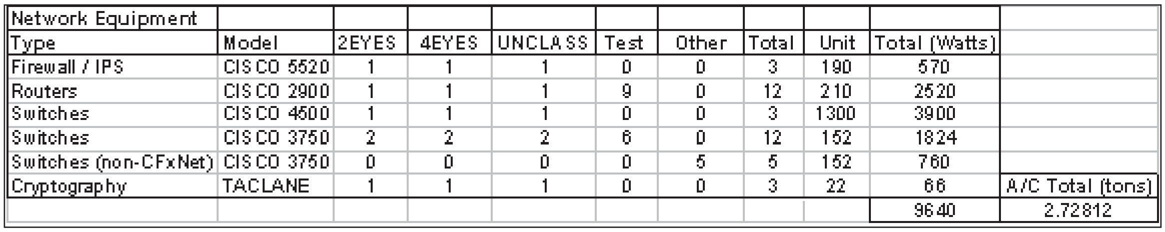
1 Watt (W)	0.000283 tons (refrigeration)
1 British Thermal Unit (BTU)	3.412141633 W
1 Kilovolt Ampere (kVA)	1111.11 W

5.1 Network Equipment Power Requirements

As discussed in the breakdown given above, five different network equipment categories are proposed for the MCEL project. These categories either refer to a security caveat, a test network application or another application.

Table 2 lists all of the network equipment to be used within the MCEL along with its published specifications for power utilization and heat. By taking a basic sum of the utilizations of all components, we obtain a basic estimate for all of the network equipment for the proposed breakdown of the MCEL.

Table 2: Power and Cooling Requirements for MCEL Network Equipment



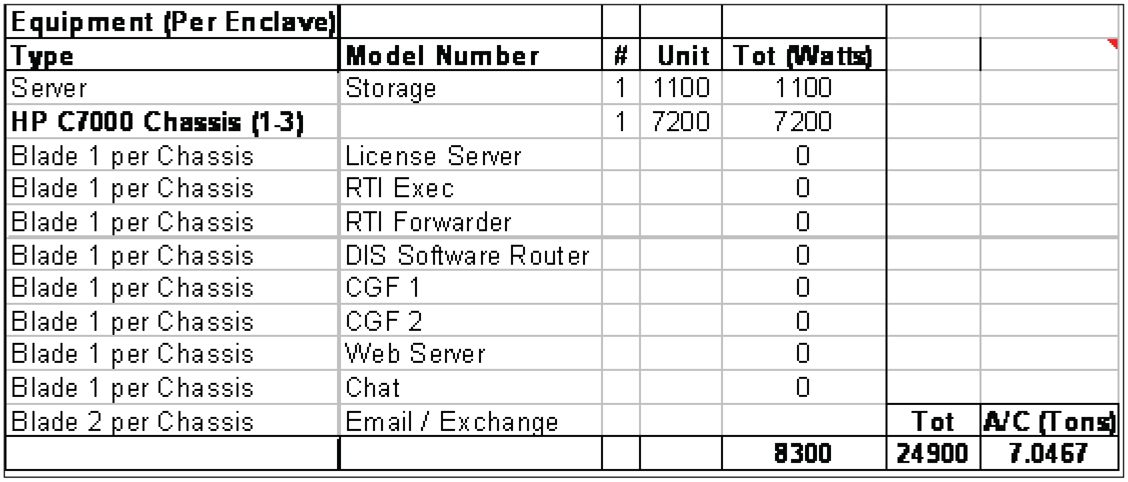
Network Equipment										
Type	Model	2EYES	4EYES	UNCLASS	Test	Other	Total	Unit	Total (Watts)	
Firewall / IPS	CISCO 5520	1	1	1	0	0	3	190	570	
Routers	CISCO 2900	1	1	1	9	0	12	210	2520	
Switches	CISCO 4500	1	1	1	0	0	3	1300	3900	
Switches	CISCO 3750	2	2	2	6	0	12	152	1824	
Switches (non-CFxNet)	CISCO 3750	0	0	0	0	5	5	152	760	
Cryptography	TACLANE	1	1	1	0	0	3	22	66	A/C Total (tons)
									9640	2.72812

While this is intuitively correct, it should be noted that not all equipment can easily be co-located without consideration of the minimum separation requirements for classified vs. unclassified network equipment. In addition, the location of the main enclave switches (i.e. Cisco 4500s) is likely to be with the servers and not necessarily with the rest of the network equipment. This therefore will impose additional restrictions on the location of these switches depending upon the security caveat to which they belong. While these considerations do not affect the final totals for electrical power requirements and cooling, they do present a number of important design decisions that must be made prior to the acquisition of any hardware or the building of any target rooms.

5.2 Simulation Equipment Power Requirements

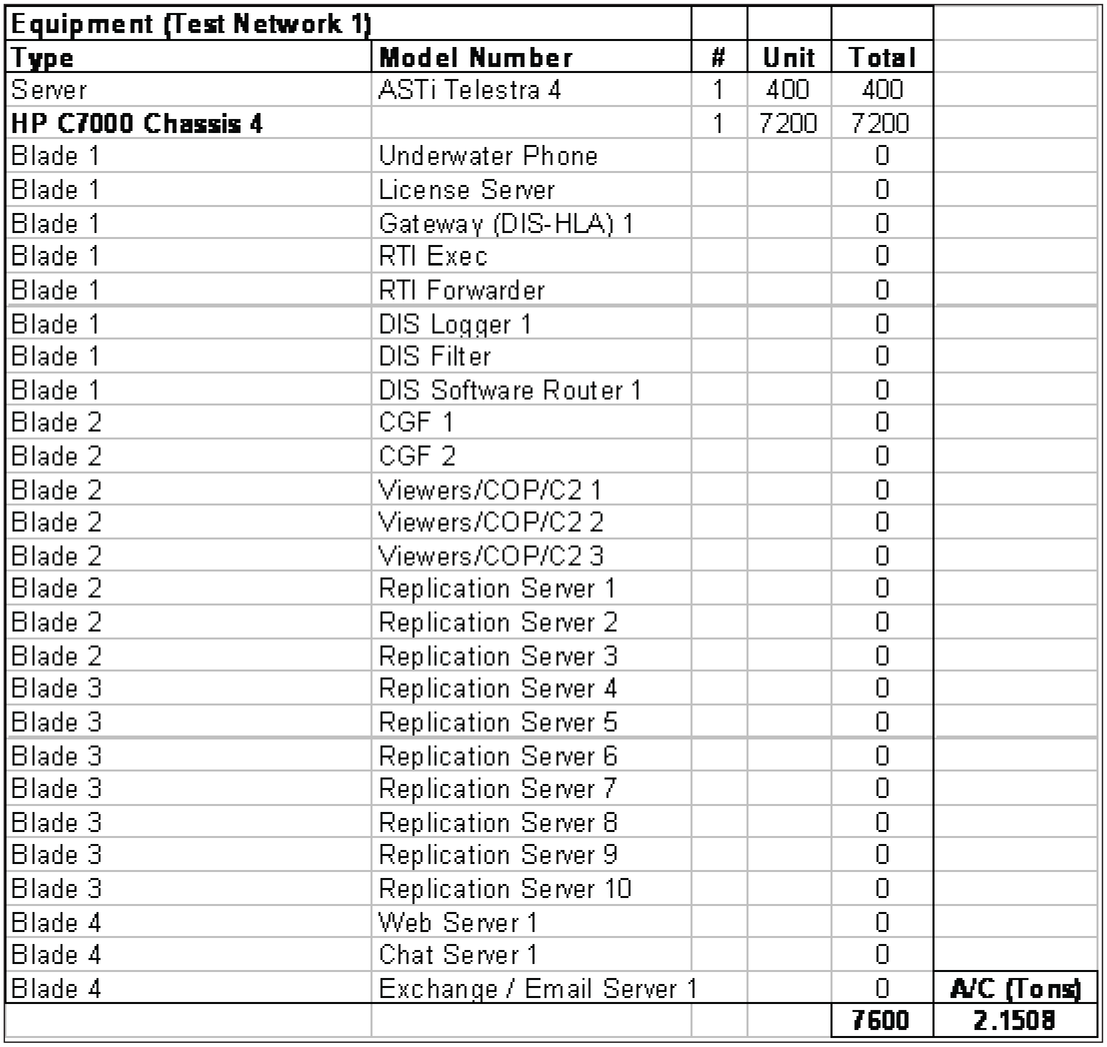
The simulation equipment outlined in the above breakdown was separated on the basis of security caveat (enclave), test network and simulation platform. While this was a logical delineation based upon the MCEL SOR and previous experience in setting up a data centre, these lines are not fixed and should allow for overlap of hardware. Tables 3-7 outline the breakdown of all of the simulation equipment for the MCEL.

Table 3: Enclave Power and Cooling Requirements for the MCEL Project



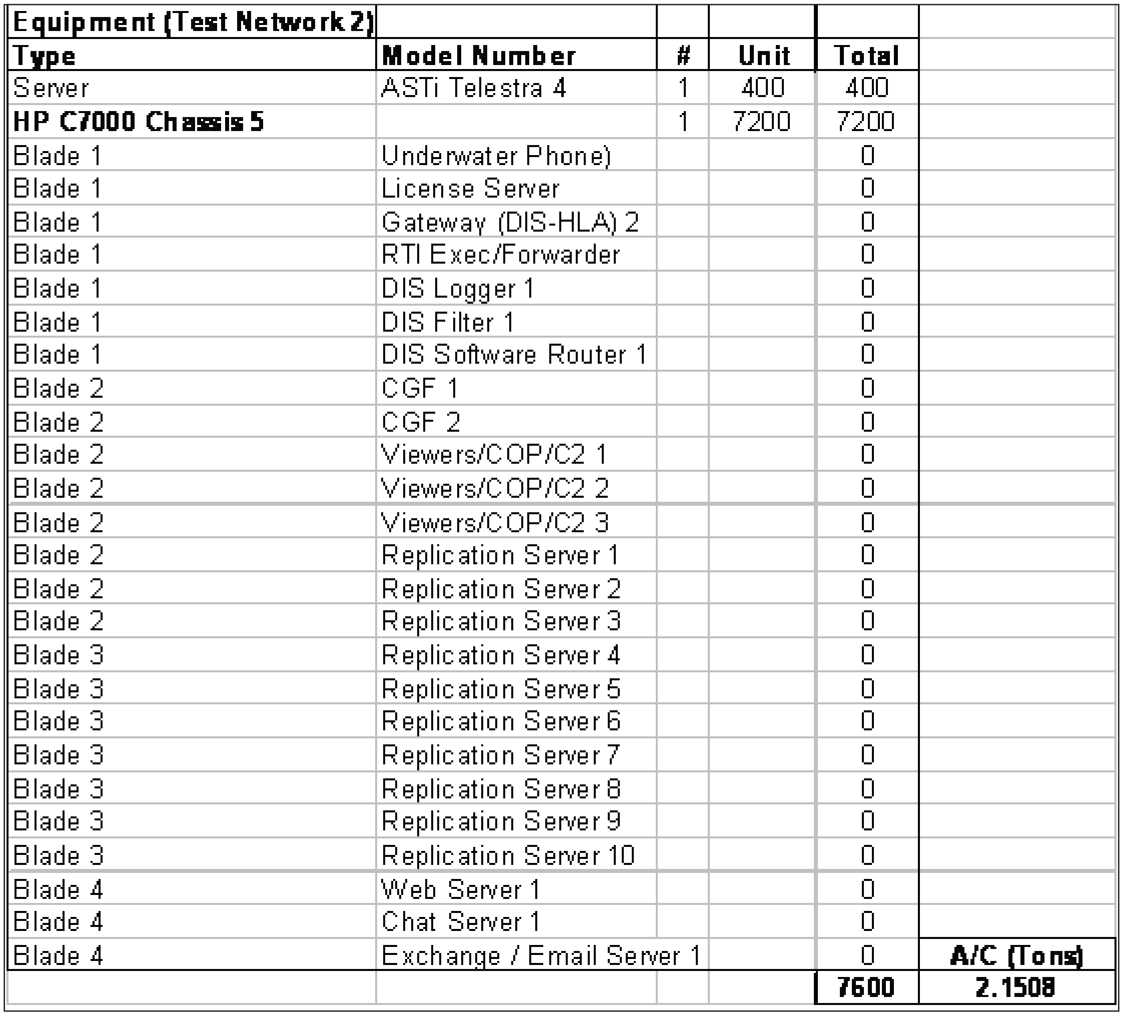
Equipment (Per Enclave)						
Type	**Model Number**	**#**	**Unit**	**Tot (Watts)**		
Server	Storage	1	1100	1100		
HP C7000 Chassis (1-3)		1	7200	7200		
Blade 1 per Chassis	License Server			0		
Blade 1 per Chassis	RTI Exec			0		
Blade 1 per Chassis	RTI Forwarder			0		
Blade 1 per Chassis	DIS Software Router			0		
Blade 1 per Chassis	CGF 1			0		
Blade 1 per Chassis	CGF 2			0		
Blade 1 per Chassis	Web Server			0		
Blade 1 per Chassis	Chat			0		
Blade 2 per Chassis	Email / Exchange				**Tot**	**A/C (Tons)**
				8300	**24900**	**7.0467**

Table 4: Test Network 1 – Power and Cooling Requirements



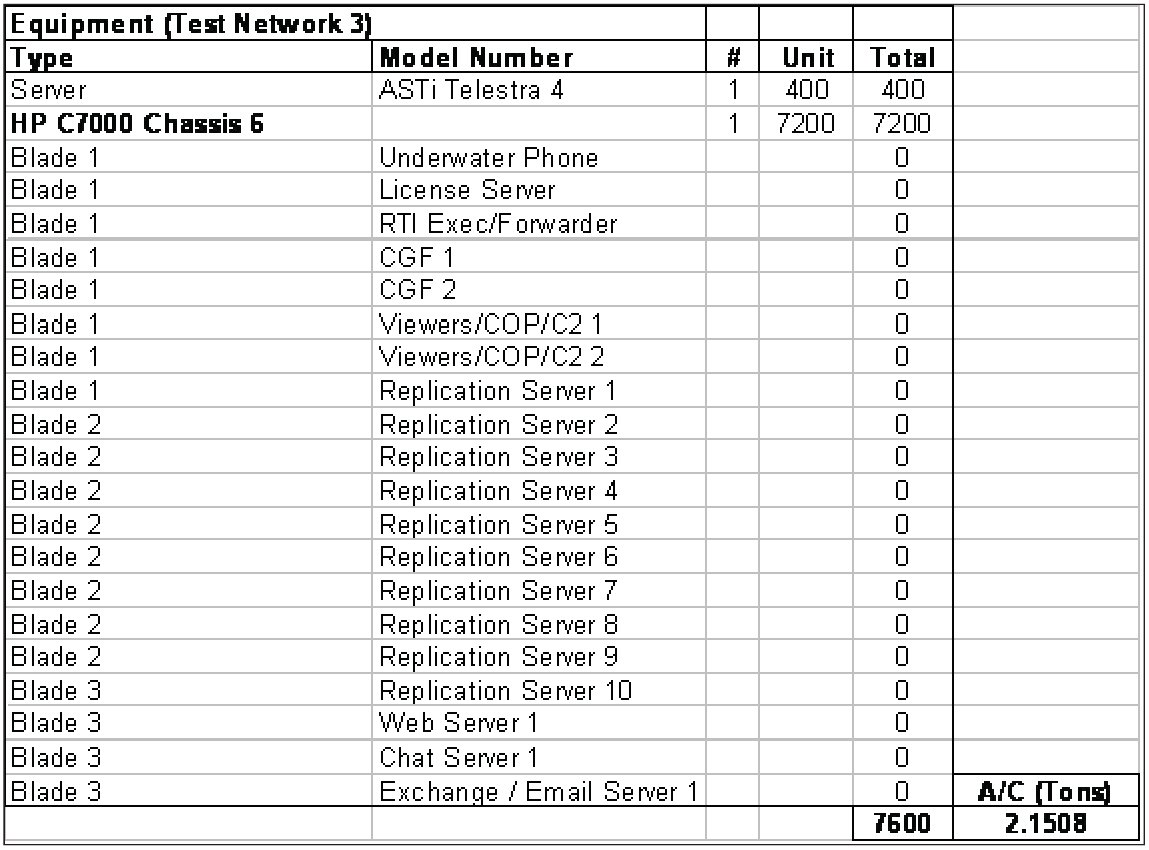
Equipment (Test Network 1)					
Type	**Model Number**	**#**	**Unit**	**Total**	
Server	ASTi Telestra 4	1	400	400	
HP C7000 Chassis 4		1	7200	7200	
Blade 1	Underwater Phone			0	
Blade 1	License Server			0	
Blade 1	Gateway (DIS-HLA) 1			0	
Blade 1	RTI Exec			0	
Blade 1	RTI Forwarder			0	
Blade 1	DIS Logger 1			0	
Blade 1	DIS Filter			0	
Blade 1	DIS Software Router 1			0	
Blade 2	CGF 1			0	
Blade 2	CGF 2			0	
Blade 2	Viewers/COP/C2 1			0	
Blade 2	Viewers/COP/C2 2			0	
Blade 2	Viewers/COP/C2 3			0	
Blade 2	Replication Server 1			0	
Blade 2	Replication Server 2			0	
Blade 2	Replication Server 3			0	
Blade 3	Replication Server 4			0	
Blade 3	Replication Server 5			0	
Blade 3	Replication Server 6			0	
Blade 3	Replication Server 7			0	
Blade 3	Replication Server 8			0	
Blade 3	Replication Server 9			0	
Blade 3	Replication Server 10			0	
Blade 4	Web Server 1			0	
Blade 4	Chat Server 1			0	
Blade 4	Exchange / Email Server 1			0	**A/C (Tons)**
				7600	**2.1508**

Table 5: Test Network 2 – Power and Cooling Requirements



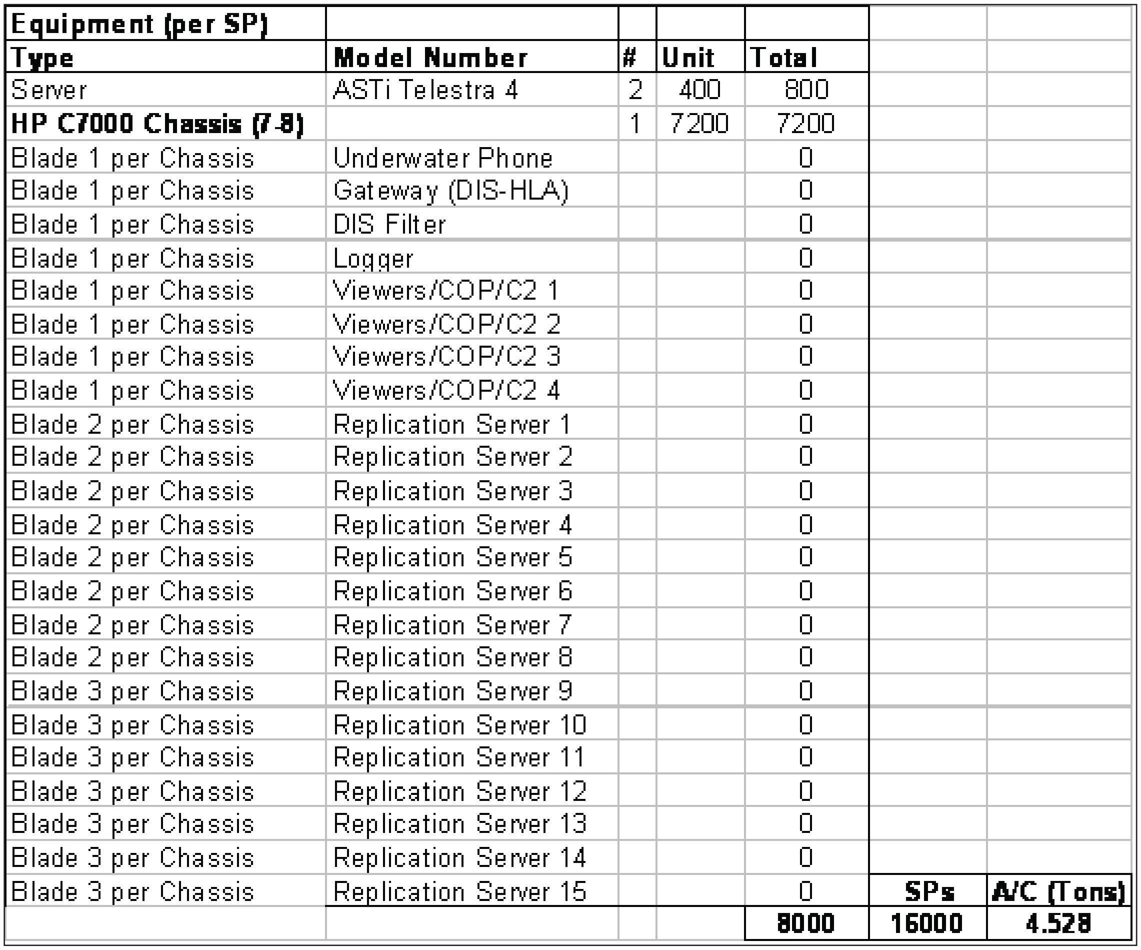
Equipment (Test Network 2)					
Type	**Model Number**	**#**	**Unit**	**Total**	
Server	ASTi Telestra 4	1	400	400	
HP C7000 Chassis 5		1	7200	7200	
Blade 1	Underwater Phone)			0	
Blade 1	License Server			0	
Blade 1	Gateway (DIS-HLA) 2			0	
Blade 1	RTI Exec/Forwarder			0	
Blade 1	DIS Logger 1			0	
Blade 1	DIS Filter 1			0	
Blade 1	DIS Software Router 1			0	
Blade 2	CGF 1			0	
Blade 2	CGF 2			0	
Blade 2	Viewers/COP/C2 1			0	
Blade 2	Viewers/COP/C2 2			0	
Blade 2	Viewers/COP/C2 3			0	
Blade 2	Replication Server 1			0	
Blade 2	Replication Server 2			0	
Blade 2	Replication Server 3			0	
Blade 3	Replication Server 4			0	
Blade 3	Replication Server 5			0	
Blade 3	Replication Server 6			0	
Blade 3	Replication Server 7			0	
Blade 3	Replication Server 8			0	
Blade 3	Replication Server 9			0	
Blade 3	Replication Server 10			0	
Blade 4	Web Server 1			0	
Blade 4	Chat Server 1			0	
Blade 4	Exchange / Email Server 1			0	**A/C (Tons)**
				7600	**2.1508**

Table 6: Test Network 3 – Power and Cooling Requirements



Equipment (Test Network 3)					
Type	**Model Number**	**#**	**Unit**	**Total**	
Server	ASTi Telestra 4	1	400	400	
HP C7000 Chassis 6		1	7200	7200	
Blade 1	Underwater Phone			0	
Blade 1	License Server			0	
Blade 1	RTI Exec/Forwarder			0	
Blade 1	CGF 1			0	
Blade 1	CGF 2			0	
Blade 1	Viewers/COP/C2 1			0	
Blade 1	Viewers/COP/C2 2			0	
Blade 1	Replication Server 1			0	
Blade 2	Replication Server 2			0	
Blade 2	Replication Server 3			0	
Blade 2	Replication Server 4			0	
Blade 2	Replication Server 5			0	
Blade 2	Replication Server 6			0	
Blade 2	Replication Server 7			0	
Blade 2	Replication Server 8			0	
Blade 2	Replication Server 9			0	
Blade 3	Replication Server 10			0	
Blade 3	Web Server 1			0	
Blade 3	Chat Server 1			0	
Blade 3	Exchange / Email Server 1			0	**A/C (Tons)**
				7600	**2.1508**

Table 7: Enclave Power and Cooling Requirements



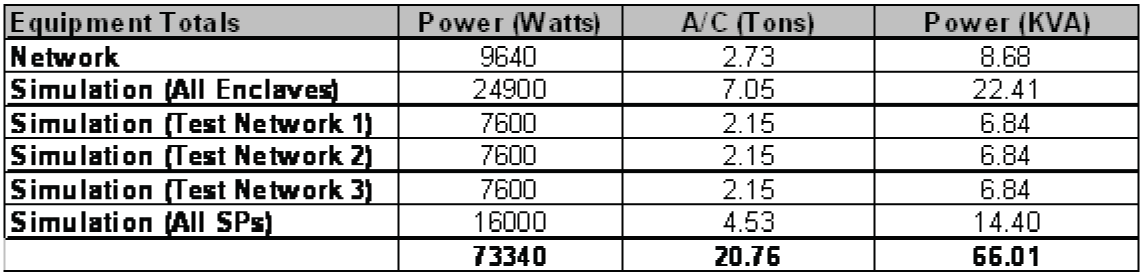
Equipment (per SP)						
Type	**Model Number**	**#**	**Unit**	**Total**		
Server	ASTi Telestra 4	2	400	800		
HP C7000 Chassis (7-8)		1	7200	7200		
Blade 1 per Chassis	Underwater Phone			0		
Blade 1 per Chassis	Gateway (DIS-HLA)			0		
Blade 1 per Chassis	DIS Filter			0		
Blade 1 per Chassis	Logger			0		
Blade 1 per Chassis	Viewers/COP/C2 1			0		
Blade 1 per Chassis	Viewers/COP/C2 2			0		
Blade 1 per Chassis	Viewers/COP/C2 3			0		
Blade 1 per Chassis	Viewers/COP/C2 4			0		
Blade 2 per Chassis	Replication Server 1			0		
Blade 2 per Chassis	Replication Server 2			0		
Blade 2 per Chassis	Replication Server 3			0		
Blade 2 per Chassis	Replication Server 4			0		
Blade 2 per Chassis	Replication Server 5			0		
Blade 2 per Chassis	Replication Server 6			0		
Blade 2 per Chassis	Replication Server 7			0		
Blade 2 per Chassis	Replication Server 8			0		
Blade 3 per Chassis	Replication Server 9			0		
Blade 3 per Chassis	Replication Server 10			0		
Blade 3 per Chassis	Replication Server 11			0		
Blade 3 per Chassis	Replication Server 12			0		
Blade 3 per Chassis	Replication Server 13			0		
Blade 3 per Chassis	Replication Server 14			0		
Blade 3 per Chassis	Replication Server 15			0	**SPs**	**A/C (Tons)**
				8000	**16000**	**4.528**

By taking the sum of all of these power requirements, we can generate an estimate of the power requirements of all of the MCEL equipment as given in our breakdown. Table 8 shows this summation and gives the required cooling requirement estimate for the building air conditioning systems.

5.3 UPS Requirements

Based upon the power totals derived from the tables above, we are able to generate an estimate of the level of UPS coverage as well as type for all of the MCEL equipment (Table 8).

Table 8: Total Power and Cooling Requirements for MCEL Equipment



Equipment Totals	Power (Watts)	A/C (Tons)	Power (KVA)
Network	9640	2.73	8.68
Simulation (All Enclaves)	24900	7.05	22.41
Simulation (Test Network 1)	7600	2.15	6.84
Simulation (Test Network 2)	7600	2.15	6.84
Simulation (Test Network 3)	7600	2.15	6.84
Simulation (All SPs)	16000	4.53	14.40
	73340	**20.76**	**66.01**

The overall power demand is approximately 66 KVA before UPS. This amount necessitates a large UPS structure which will contain multiple racks. The demand on this UPS would be spread over several rooms and thus an in-depth design would be required. This could be mitigated by having rack mounted UPS for the network rooms and, based on estimated loads, this is what we recommend. Based on our estimated load for the server room and our rack assignment, the server room load could also be accomplished via rack mounted UPS although this is not necessarily the best path. Selection of the best UPS design should be a consultative process with the electrical designers for the MCEL project as well as DIMTPS staff. Our option, proposed below, is one way to provide battery backup based on no building design input and no in-depth analysis of whether battery backup is required for all devices, a subset of the devices or even at all. Battery backup would aid in preventing the dropping of network connections during power spikes and short outages however they would not provide sufficient power to continue running an experimentation/exercise and so should be viewed in that light as giving the ability to safely shut down servers and storage devices during a power outage.

As discussed above, if we were to break-up the network equipment more logically to account for separation of classified vs. unclassified equipment as well as remove the main enclave switches from the network equipment and move it among the servers, the above requirements would change as follows:

Table 9: Power and Cooling Requirements for MCEL UNClass Networks

Power (Watts)	A/C (Tons)	Power (KVA)
970	0.275	0.873

Table 10: Power and Cooling Requirements for MCEL Classified Networks

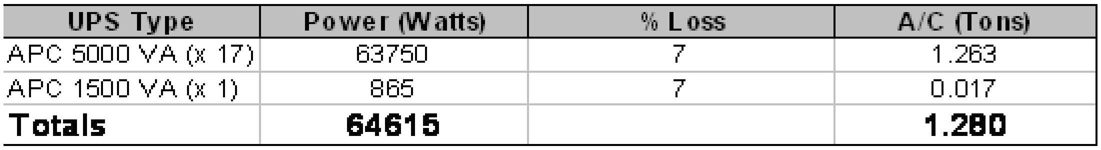
Power (Watts)	A/C (Tons)	Power (KVA)
4770	1.350	4.293

For the unclassified network room, we would have an equipment load of approximately 1KVA which would necessitate a 1500VA UPS to provide battery backup of limited duration. Similarly, the classified network room would have an equipment load of approximately 4.3 KVA which would necessitate 5000VA UPS to provide battery backup of a limited duration.

By further examining Table 8, we can also determine that each enclave, test network and simulation platform requires between 6KVA – 8KVA (2x 5000VA UPS backups). A simple breakdown of the total UPS requirement is given in Table 11.

While this is a simplified breakdown, it should be noted that a mix of different types of UPS backup strategies may be needed – A Blade chassis will likely require a dedicated UPS and adding a second smaller UPS to support specialty servers (i.e. Telestra 4) would be the ideal. The ideal UPS(s) should be determined when the server equipment (Blade vs. std server) philosophy is decided and post a review of whether SPs are fixed within security enclaves or not. Based upon our assessment, a total of 17 5KVA UPS units and a single 1.5KVA UPS unit would be necessary to support all of the MCEL equipment defined in the current breakdown. We have chosen to use the APC 5000 KVA and APC 1500 KVA UPSs as representative for our calculations.

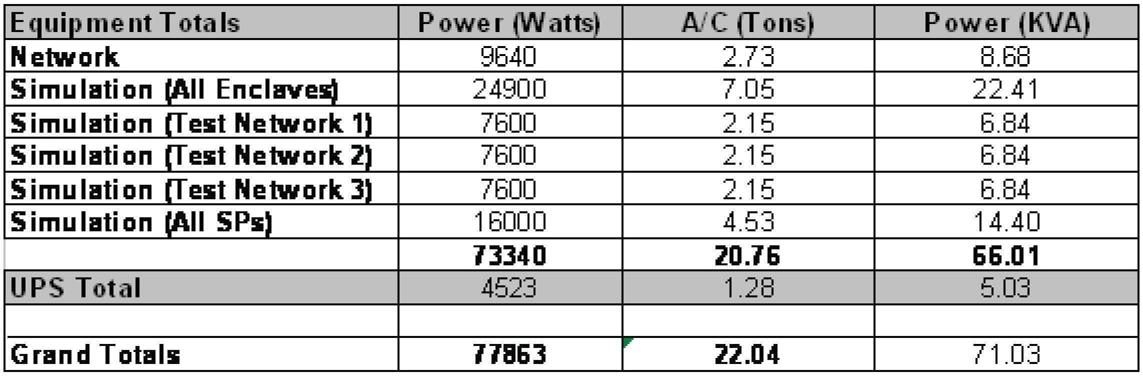
Table 11: UPS Power and Cooling Requirements



UPS Type	Power (Watts)	% Loss	A/C (Tons)
APC 5000 VA (x 17)	63750	7	1.263
APC 1500 VA (x 1)	865	7	0.017
Totals	**64615**		**1.280**

Based upon the manufacturer's rating of a 93% efficiency (i.e. 7% loss), we can reformat Table 8 to include the electric power requirement for the entire MCEL including the UPS backup as follows. These updated values are reflected in Table 12.

Table 12: Power and Cooling Requirements for the MCEL Project



Equipment Totals	Power (Watts)	A/C (Tons)	Power (KVA)
Network	9640	2.73	8.68
Simulation (All Enclaves)	24900	7.05	22.41
Simulation (Test Network 1)	7600	2.15	6.84
Simulation (Test Network 2)	7600	2.15	6.84
Simulation (Test Network 3)	7600	2.15	6.84
Simulation (All SPs)	16000	4.53	14.40
	73340	**20.76**	**66.01**
UPS Total	4523	1.28	5.03
Grand Totals	**77863**	**22.04**	71.03

From the above table, we observe that an air conditioning system capable of providing a minimum of 22.04 tons of cooling is required to support the current hardware configuration of the MCEL project as given in the breakdown. It is also seen that the facility housing the MCEL would need to provide a minimum of approximately 78 KWh for its proper operation. While this cooling figure represents the minimum load, it should be noted that this equipment will likely be spread across a number of rooms and therefore this threshold could be met through the use of a number of A/C systems combined. In addition, the expectation is that the MCEL will grow and so a refinement of the requirements is recommended where a growth strategy can be factored in.

6 Noise Dampening Strategies

Noise can be defined as unwanted sound. Within a server/network room noise tends to be generated by the fans contained within computer/network equipment and by the HVAC system. This noise is generated over a wide range of frequencies due to the difference between fans and due to the turbulent airflow created by the fans. There are several strategies that can be employed to reduce the effects of noise. Some of these strategies are dependent upon whether you are trying to reduce the noise externally or to reduce the noise internally while some strategies support both.

6.1 External Noise Reduction

The following lists a variety of external noise reduction strategies:

1. **Location of room**. During building design the network/server rooms should be sited to minimize the impact of their inherent noise. This means not locating these rooms adjacent/near to office cubicles or meeting rooms. Where possible, site network/server rooms near mechanical rooms, janitorial rooms, storage rooms etc. This has the potential benefit of allowing server racks to be moved closer to the wall while still maintaining security separation provided it can be demonstrated that no electronic equipment can be sited on the outside wall of the network/server room.

2. **Flooring**. Network/server room can be either a solid floor or a raised floor. A solid floor will not have any soundproofing applied to it however will be sufficiently dense to provide sufficient noise reduction. An anti-static material should be applied to the floor. A raised floor will allow for HVAC cooling to be directed into the cold aisles. This raised space will aid in noise reduction.

3. **Walls & Ceiling**. If location of the network/server room is insufficient to mitigate concerns over noise then sound barrier insulation can be integrated with the walls & ceiling. There is a variety of sound barrier insulation (i.e. Sonex) available. Sound barriers seen in network/server rooms tend to be acoustic ceiling tiles as well as either treating existing walls with acoustical foam or mounting acoustic panels on the walls.

6.2 Internal Noise Reduction

The following lists a variety of internal noise reduction strategies:

1. Application of sound barrier insulation on ceilings and walls reduce the noise internally primarily through sound absorption (reduction of sound reflecting off the hard flat surfaces of the walls, dropped ceiling).

2. Minimizing the time spent in network/server room will decrease the impacts of the noise levels contained within the respective rooms. This is not meant as a glib statement. All equipment within the network/server room should be able to be remotely accessed. What is critical is that only those with the requisite authorities can access this equipment remotely much like the security controls in place for physical access to each room. The vast majority of the servers should be available via the Management network and thus can be powered on/off

remotely. With a remote desktop capability enabled the servers can be operationally controlled via a remote client on the appropriate operational or test network.

3. Headsets could also be worn within the confines of the network/server room. These headsets could range from simple hearing protection up to Active Noise Cancelling headsets.

References

Diminico, C (2006). Telecommunications Infrastructure Standard for Data Centers: ANSI/TIA-942. Retrieved March 20, 2012 from IEEE 802 organization Web Site: http://www.ieee802.org/3/hssg/public/nov06/diminico_01_1106.pdf.

Hewlett Packard (2012). HP BladeSystem c7000 Enclosures – overview. Retrieved March 20, 2012 from HP Web Site: http://h18004.www1.hp.com/products/blades/components/enclosures/c-class/c7000/.

Nye, H., Benedetti, R (2000). American Power Conversion (APC): Power Factor Correction: Changing your power needs. Retrieved March 20, 2012 from the APC resources Web Site: http://www.apc.com/resource/pdf/silconwhite.pdf.

TIA (2005), Telecommunications Infrastructure Standard for Data Centres: TIA_942. Retrieved March 20, 2012 from http://dc.uni.ru/norms/tia942.pdf.

Unit Conversion Organization (2009). Power Converter: Online Tool. Retrieved/Utilized March 20-29, 2012 from http://www.unitconversion.org/unit_converter/power.html.

[1] Defence Research and Development Canada – ADM(S&T) (2011). MARITIME SCIENCE AND TECHNOLOGY EXPERIMENTATION CAPABILITY PROJECT – Maritime Capability Evaluation Laboratory (MCEL): Statement of Operational Requirement (SOR), DSP NO 00001671.

[2] Cisco. Campus Network for High Availability Design Guide – Cisco Validated Design I. Retrieved March 20, 2012 from Cisco Web Site: http://www.cisco.com/application/pdf/en/us/guest/netsol/ns431/c649/ccmigration_09186a008093b876.pdf.

[3] Hucaby, D., Garneau, D., Sequeira, A. (2011). *CCNP Security FIREWALL 642-617 Official Cert Guide*. (1st ed.), Indianapolis (IN): CiscoPress.

[4] Welkins, S. (2011). *Designing for Cisco Internetwork Solutions (DESGN) Foundation Learning Guide*. (3rd ed.), Indianapolis (IN): CiscoPress.

This page intentionally left blank.

List of symbols/abbreviations/acronyms/initialisms

2Eyes	Canada/USA
4Eyes	Australia, Canada, United Kingdom and United States of America
AAR	After Action Review
AC	Air Conditioning
AFB	Air Force Base (USAF)
ANSI	American National Standards Institute
ASTi	Advanced Simulation Technologies Inc.
BIOS	Basic Input/Output System
BTU	British Thermal Unit
C2	Command & Control
CAN/CSA	Canadian Standards Association
CASE	Canadian Advanced Synthetic Environment
CF	Canadian Forces
CFBLNet	Combined Federated Battle Laboratories Network
CFXNet	Canadian Forces Experimental Network
CFWC	Canadian Forces Warfare Centre
COP	Common Operating Picture
CPU	Central Processing Unit
CSNI	Consolidated Secret Network Infrastructure
DIMTPS	Director Information Management Technologies, Products and Services
DIS	Distributed Interactive Simulation
DMZ	De-Militarized Zone
DND	Department of National Defence
DRDC	Defence Research and Development Canada
DRENet	Defence Research Network
DSP	Digital Signal Processing
DWAN	Defence Wide Area Network
EIA	Electronic Industries Alliance
EXEC	Executive
FTP	File Transfer Protocol
GCCS-M	Global Command and Control System – Maritime
GoC	Government of Canada
GOTS	Government Off The Shelf

HLA	High Level Architecture
HP	Hewlett-Packard
IG	Image Generator
ILO	Integrated Lights Out (HP Trademark)
INFOSEC	Information Security
IOS	Internetwork Operating System
IP	Internet Protocol
ISP	Internet Service Provider
ISR	Integrated Services Router
ISSO	Information System Security Officer
IT	Information Technology
ITSG	Information Technology Security Guidance
KMM	Keyboard, Mouse, Monitor
KVA	Kilo Volt-Amperes
LAN	Local Area Network
MCEL	Maritime Capability Evaluation Laboratory
M&S	Modelling and Simulation
NAS	Network Attached Storage
NATO	North Atlantic Treaty Organization
NSTISSI	National Security Telecommunications and Information Systems Security Instructions
OA	Operational Authority
OOB	Out of Band
PC	Personal Computer
PDU	Protocol Data Unit
POE	Power over Ethernet
RCN	Royal Canadian Navy
RFC	Request for Change
RTI	Run Time Infrastructure
SAN	Storage Area Network
SFP	Small Form-factor Pluggable (Transceiver)
SP	Simulation Platform
T4	Telestra 4 (server)
TA	Technical Authority

TBITS	Treasury Board Information or Technology Standard
TELCO	Telecommunications
TIA	The Telecommunications Industry Association
TRL	Technology Readiness Level
Unclass	Unclassified Security Caveat
UPS	Uninterruptible Power Supply
USAF	United States Air Force
USB	Universal Serial Bus
USN	United States Navy
VLAN	Virtual Local Area Network
VOIP	Voice over IP
WAN	Wide Area Network